
30 Internet Fundamentals and Cyber Security Management

HURA GURDEEP

INTRODUCTION

Since its inception and wide acceptance, the Internet has revolutionized our society, our economy, and many of our technological systems. No one knows for certain how far, or in what direction, the Internet will evolve. But no one should underestimate its importance in creating new applications and technologies.

Over the past century and a half, important technological developments in various disciplines have created a global environment that is drawing the people of the world closer and closer together, for example, transportation, person-to-person communication, mutual understanding of culture, trading, and many other avenues. During the industrial and manufacturing revolutions, we learned to put motors to work to magnify human and animal muscle power. In the new information technology age, we are learning to magnify brainpower by using the power of computation and data interpretation wherever we need it and to provide information exchange services on a global basis. Computer resources (e.g., processing units, memory devices, and various peripheral devices) are infinitely flexible tools and are networked together, allowing us to generate, exchange, share, and manipulate information in an uncountable number of ways. The Internet, as an integrating force in today's information technology age, has melded the technology of communications, internetworking, client-server, and computing to provide instant connectivity and global information services to all its users at a reasonable cost.

WHAT IS INTERNET?

In 1982, the earliest definition of Internet was stated to be a global system that interconnects various computer networks and uses standard Internet Communication Protocol suite (Transmission Control Protocol/Internet Protocol [TCP/IP]). It can also be defined as network of networks that consists of millions of private and public, academic, business, and government networks for local and global communication. These networks are connected by a variety of communication media like twisted pair of copper wires, fiber-optics, cables,

microwave, satellite and wireless, and other new technologies. The procedures by which computers communicate with each other are called "protocols." A protocol consists of three components as syntax (structure or format of the data in bits), semantics (meaning of each aspect of bit), and timing (when and how fast data should be sent). While this infrastructure is steadily evolving to include new capabilities, the protocols initially used by the Internet are called the "TCP/IP" protocols, named after the two protocols that formed the principal basis for Internet operation. Some of the material presented here have been derived from Refs. [1–5].

At the highest level of abstraction, the Internet is a network of interconnected networks comprised of a myriad of host computer systems joined together by communications links (wired and wireless). Host computer systems communicate by sending messages to each other over the communication links, where a standard network protocol suite called TCP/IP specifies the data formats and transmission rules. Looking at a greater level of detail, one sees that the Internet is a *packet-switched* network. Messages to be transmitted across the Internet are broken into manageable chunks called *IP packets*, which contain the data to be sent (such as part of an electronic mail (e-mail) message or web-page content); the *destination* address (i.e., the "TO" field); the *source* address (i.e., the "FROM" field); a *port* number (which represents a specific type of service offered by a host, such as mail transfer, file transfer, or web browsing); and other miscellaneous header information that supports the reliable transmission of data. A vast array of network devices called *routers* forward each packet, so that it moves from router to router until it arrives at its desired destination, or until the number of routers touched by the packet exceeds a maximum allowed value.

The Internet (originally known as ARPANET) began its life in 1969 as a research network (based on newly developed packet switching concepts) sponsored by the Advanced Research Projects Agency (ARPA) of the Department of Defense (DoD). By the end of that year, the ARPANET consisted of four nodes, connecting four U.S. universities (University of Southern California [UCLA], Stanford Research Institute [SRI], the University of California, Santa Barbara [UCSB], and the University of Utah) via interface message processor to form a network. The communication

between these connected hosts was provided by network control protocol. By 1973, the first international connections to the ARPANET were made to selected NATO countries via NORSAR. At that time, the ARPANET was essentially the only realistic wide-area computer network in existence, with a base of several dozen organizations.

Prof. Cerf's group at Stanford were involved in the initial detailed design of the TCP software under DARPA contract and, shortly thereafter, with Bolt Beranek and Newman (BBN) and University College London to build independent implementations of the TCP protocol (as it was then called—it was later split into TCP and IP) for different machines. BBN also had a contract to build a prototype version of the gateway. These three groups worked together for the development and testing of the initial communication protocols on different machines. Prof. Cerf, provided the day-to-day leadership in the initial TCP software design and testing. BBN deployed the gateways between the ARPANET and the PRNET and also with SATNET. During this period, under Kahn's overall leadership at DARPA, the initial feasibility of the Internet architecture was demonstrated.

The infrastructure is an emerging set of architectural concepts and data structures for heterogeneous information systems that has made the Internet a truly global information system. The architecture concepts can be implemented viewing two different abstractions. In one abstraction, we may view it as a system that deals with connectivity, communications packet delivery, and a variety of end–end communication services between two hosts. The other abstraction assumes the Internet as an information system, independent of its underlying communications infrastructure that allows creation, storage, transparency, and easy access to a wide

range of information resources, including digital objects and related services at various levels of abstraction.

EVOLUTION OF INTERNET

There are two main technologies and research efforts that led to Internet, *packet switching* and *computer technology*, which, in turn, drew upon the underlying technologies of digital communications and semiconductors. The research efforts were able to demonstrate the possibility of sharing of information and computational resources over the Internet. During this time, ARPANET was taken over by Defense Communication Agency (DCA). In October 1977, three networks ARPANET, PRNET, and SATNET were connected and were able to communicate with each other. Some of the information presented here is derived from Refs. [2–7].

The Internet standards describe a layered model/framework of IP suite (TCP/IP) as shown in Figure 30.1. Each of the layers in the model describes a specific services and functionalities. The TCP/IP model is designed in such a way that it offers connectivity to all underlying hardware and as does not include the details. The top layer of protocol architecture is an application layer that defines application-specific methods used in software applications, for example, browser program, mail program, file-transfer program, remote logon program, etc. The transport layer below application layer provides connectivity to applications on different hosts via the client–server model with appropriate data exchange techniques. TCP manages higher level functions in the layered model such as segmentation, reassembly, and error detection. IP on other handle manages datagram routing within the Internet.

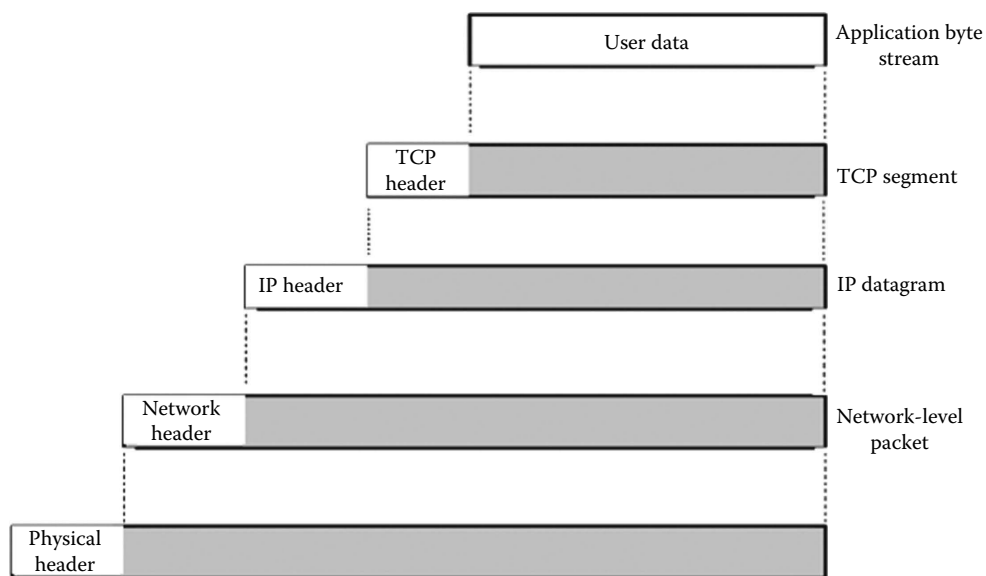


FIG. 30.1
TCP/IP protocol architecture.

TABLE 30.1

Comparison of OSI, IEEE 802 Model, and TCP/IP Protocol Architecture

<i>OSI</i>	<i>IEEE 802 Model</i>	<i>TCP/IP</i>
Application	Application	Application
Presentation	Presentation	
Session	Session	Transport (host-to-host)
Transport	Transport	
Network	Network	Internet
Data link	LIC MAC	Network access
Physical	Physical	Physical

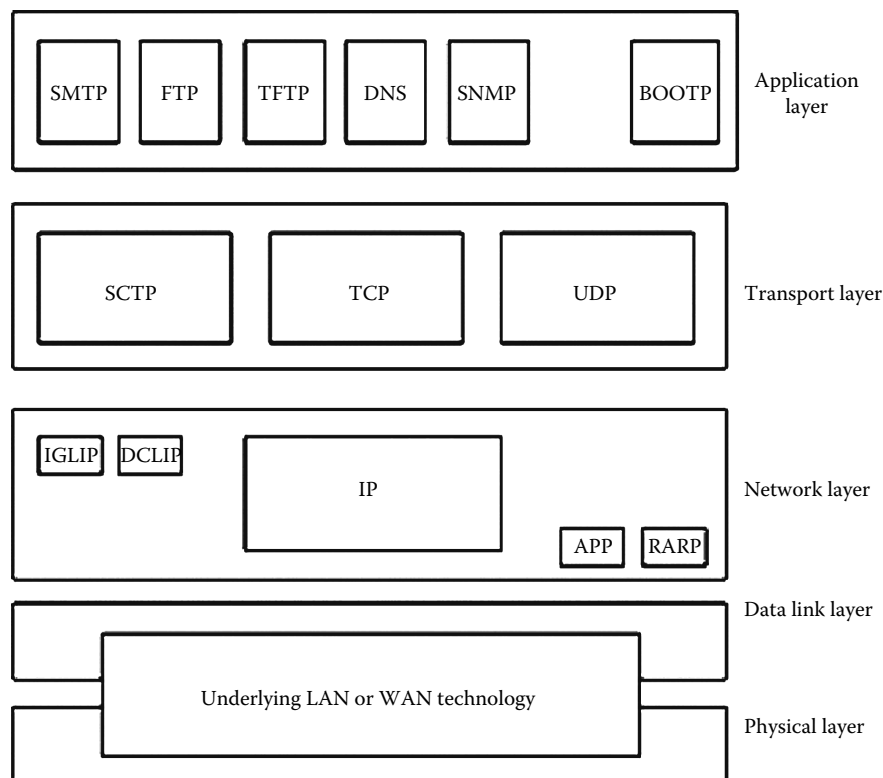
The underlying two layers Internet and Link represent the network technologies. The Internet layer using IP enables computers to identify, locate, and connect to one-another via intermediate networks. The link layer provides connectivity between hosts on the same networks, for example, local area network (LAN) or dial-up connection. Other models have been developed, such as the open systems interconnection (OSI) model, but they are not compatible in the details of description, or implementation, but many similarities exist and the TCP/IP protocols are usually included in the discussion of OSI networking. A comparison of TCP/IP, OSI-reference model, and IEEE models based on layered concept is shown in Table 30.1. Figure 30.2 shows a list of protocols

that are being defined and supported by each of the layers of TCP/IP architecture.

The IP used in network layer plays a very important role as it provides addressing systems (IP addresses) for computers on the Internet and as such enables internetworking and essentially establishes the Internet itself. The first version of IP is IP version 4 (IPv4), which is still in dominant use in today's Internet. It was designed to address up to ~4.3 billion (10^9) Internet hosts.

Many individuals have been involved in the development and evolution of the Internet, covering a span of almost four decades on the subject of computer networking by Kleinrock, Licklider Baran, Roberts, and Davies. The ARPANET, was the first wide-area computer network. The NSFNET, which followed more than a decade later under the leadership of Erich Bloch, Gordon Bell, Bill Wulf, and Steve Wolff, brought computer networking into the mainstream of the research and education communities. A readable summary on the history of the Internet, written by many of the key players, may be found at Refs. [4,7].

Internet has grown and developed significantly since 1993, in particular the concept of hypertext (that links the information contained in different computers) proposed by CERN scientists Tim Berners-Lee and Robert Cailliau in 1989. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support e-mail. The first Internet browser

**FIG. 30.2**

Protocols for TCP/IP architecture.

(a program that allows access to different computers) using mouse was introduced in 1990. The first browser on a commercial scale was produced (Mosaic) in 1993 that allowed the visualization of colored pictures and images. At the same time, a user-friendly system to use the browser for looking up information called WWW was introduced.

World Wide Web

WWW is a repository of information of different areas linked together around the globe over the Internet. It offers flexibility, portability, and user-friendly features. This project was initiated by European Laboratory for Particle Physics (CERN) to develop a system for managing distributed resources through standard termed as hypertext markup language (HTML) that supports a procedure to attach to a word or phrase that links it to another document located anywhere on the Internet. The documents created by HTML are stored on servers and can include text, visual images, streaming video, audio clips, animated images, and other forms of pictures. It is based on client-server paradigm where client uses a browser to access the information from service servers located around the globe. For more details of client-server and socket implementation, readers can refer to Chapter 29.

The WWW is a global set of documents, images, and other resources, referenced and interconnected by uniform resource locators (URLs) and hyperlinks. These URLs allow users to address the web servers and other devices that store these resources and access them as required using the hypertext transfer protocol (HTTP). HTTP is only one of the communication protocols used on the Internet. Web services may also use HTTP to allow software systems to communicate in order to share and exchange business logic and data. Other services provided by Internet for person-to-person communication include: on-line chat and shopping, file sharing, file transfer, publishing, telnet, remote login, games, commerce, social networking, video-on-demand, teleconferencing, telecommunications, voice over Internet protocol (VoIP) via voice and video and many others.

The web has transformed the Internet into a user-friendly medium as it provides back-end protocols for authoring and distributing web pages (HTML and HTTP) that found banners and commercial messages in almost every region of cyberspace. In order to locate a particular site, search engines such as Google are very useful. These search engines are sometimes inefficient due to the huge amount of data they are handling. Regardless of the difficulties that users experience while navigating on the Internet, the web continues to rapidly gain in popularity. We have seen a next-generation web such as Semantic web that will understand human language and is possible due to extensive use of XML; a language that can link words and phrases so that computers can interpret. Net browsers such as Navigator offered by Netscape or Microsoft's Internet Explorer enable users explore the web easily.

Forms of Web Document

Web documents can be of different forms as static, dynamic, and active.

1. The *static* document is created with fixed content and stored in a server. HTML is being used to create this type of web document.
2. The *dynamic* document is created by server on demand by the browser. The server runs an application program or script that creates dynamic document. The Common Gateway Interface (CGI) is being used to create dynamic documents. It defines a set of standards for performing a number of operations on dynamic documents like creation, inputting and outputting of data to program, updating, etc. that any programming language has to follow. It is important to know that it is not a language, but supports different types of languages like C++, Perl, Bourne Shell, Korn Shell, C Shell, Tel. Pearl is the most popular open source web programming language. Other popular open source programming languages are: Python, Ruby, TCL/TK, PHP, and Zope. Some new technologies based on scripts have been introduced for creating dynamic document such as Hypertext Preprocessor (PHP based on Perl), Java Server Pages (JSP based on Java), Active Server Pages (ASP, a Microsoft software based on Visual Basic), ColdFusion (interleaving of SQL and HTML), etc. Highly recognized GNU compilers available and used widely for programming language like C, C++, Objective-C, Fortran, Java and ADA GNU represents not UNIX.
3. *Active* web application runs on client's machine and creates animated graphics on the screen. Java Applets are being used to create this class of web document. Applet is written in Java and runs on server as a compiled program that can be used. The concepts of scripts can also be used in the creation of web-active documents. Apache (open source software) runs about half of the world's web servers. Firefox is the most popular web browser in Europe and the second most popular web browser worldwide.

HOST CONFIGURATION

As described earlier, an Internet is an interconnection of a number of physical networks connected by internetworking devices like routers. When a source node sends a packet to the destination station, it goes through a number of connected networks and routers. The logical address at network is defined to identify the hosts and routers. The logical address in TCP/IP is known as IP address of 32 bit. The hosts and routers will also have a physical address at the physical layer as packets travel through them. The physical address is primarily a local unique address and not a global address and

usually implemented in hardware, for example, media access control (MAC, one of the sub layers of data link layer in open system interconnection reference model [OSI-RM]) address of 48-bit in Ethernet protocol that are imprinted on the network information center (NIC) installed in the host or router. Both logical and physical addresses are needed as LANs may support different protocols, for example, Ethernet may support IP and Internet packet exchange (IPX, Novel) at the same time at physical layer. Similarly, at network layer, different networks may be used such as Ethernet, LocalTalk (Apple). IPX is the original NetWare network-layer (Layer 3) protocol used to route packets through an internetwork. IPX is a connectionless datagram-based network protocol and, as such, is similar to the IP found in TCP/IP networks. Some of the material presented here is being derived from Refs. [2,4–8].

The messages are communicated as packets and are relayed from computer-to-computer until they reach their destination. The special computers that perform this forwarding function are called variously “*Packet switches*” or “*Routers*.” Together these routers and the communication links between them form the underpinnings of the Internet. The packet switching allows the packets to be delivered to the destination and uses IP to send the packets to the destination and TCP makes sure that the packets are delivered to the destination in spite of loss of packets, occurrence of errors with nodes and links, error encountered in the packets, out of order arrival of the packets, and re-sending of the packets.

The forwarding of a packet from one router to a second router is called a *hop*. Each router has a table of routing information (containing a snapshot of the network topology) that it builds and updates by communicating with other routers. The router uses this routing information in an attempt to choose the best path for sending a packet toward its desired destination. In simplest terms, a router looks at the destination address of a packet and sends the packet to another router that moves the packet closer to its final destination. Typically, there are many alternative paths to a destination, which enables packets to be routed around communications links or routers that are out of service due to attack, accident, or even maintenance. Thus, this packet-switched design allows the Internet to be robust in the face of accidents or external physical attacks on the routing infrastructure. This, in fact, was one of the original design goals of the Internet. TCP attempts to ensure that the packets are successfully delivered, in the proper order, and it will retransmit packets in the event of their loss.

TCP allows two hosts to establish a connection or a session for a period of time to exchange streams of packets to support a service such as e-mail, file transfer protocol (FTP), or web browsing (one of the header fields in the packet contains a numerical counter called time to live [TTL]), which is decremented by one for each hop (i.e., each time a router processes the packet) to prevent infinite looping. When the counter reaches zero, the packet is no longer forwarded, and a control packet (i.e., a notification) is sent back to the source address.

The Internet grew so rapidly that the names of the host computers (e.g., UCLA, USC-ISI) have to be translated into Internet addresses so that lower layer protocols could be activated to support the applications. A group at SRI International in Menlo Park, CA, known as NIC, was formed with a view to maintain a simple, machine-readable list of names and associated Internet addresses that can be used on the net. Hosts on the Internet are required to maintain a list as a local copy of the table on a regular base from “host.txt” file (since it was simply a text file). The list performs the translation of a name into an Internet address.

Each host on the Internet has an *IP address*, which allows packets to be delivered to and received from a specific host. An IP address consists of four decimal numbers in the range 0–255, separated by periods (each decimal number represents 8 bits of a 32 bit binary representation of the IP address). For example, the IP address of the computer emergency response team (CERT) Coordination Center’s web server is 192.88.209.14. However, it is clearly more mnemonic and convenient for a human to enter a name like “www.cert.org” in a web browser window than to enter a purely numeric address.

TCP/IP PROTOCOL SUITE

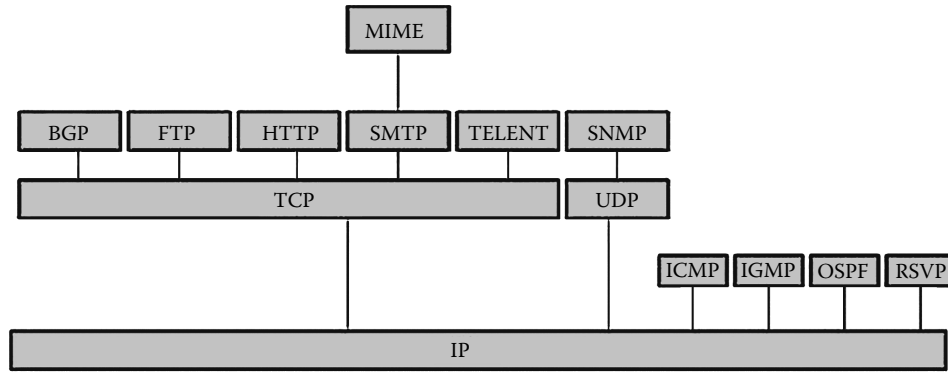
During the development of TCP/IP and other related computer technology, a variety of protocols in the TCP/IP suite were developed and were integrated in the original TCP/IP model as shown in Figure 30.3. The following section describes each of the protocol functions defined in the model. Some of the materials presented below have been derived from Refs. [2,5–11].

Any host or router connected to Internet should have IP address, subnet mask of computer and IP address of name server. This information is usually stored in a configuration file that can be accessed by computers during bootstrap process. The diskless computers use bootstrap protocol (BOOTP) that provides the above information and is based client–server paradigm. reverse address resolution protocol (RARP) also provides IP address for diskless computers but it works at data link layer and both client and server have to be on the same network. This is not required in BOOTP.

Dynamic Host Configuration Protocol (DHCP): This protocol provides static and dynamic address allocation where DHCP server maintains a database that binds to physical addresses to IP addresses.

Hypertext Transfer Protocol (HTTP): This protocol allows the user to access the web. It uses one TCP connection (on port 80) for transferring the data between client and server. It transfers the files and also provides Internet services.

Internet Control Message Protocol (ICMP): As said earlier, transport layers offers two types of services as connection-oriented (reliable via TCP) and connectionless (unreliable via user datagram protocol [UDP]). To support these, IP

**FIG. 30.3**

Protocols in the TCP/IP protocol suite. BGP, Border Gateway Protocol; FTP, File Transfer Protocol; HTTP, Hypertext Transfer Protocol; ICMP, Internet Control Message Protocol; IGMP, Internet Group Management Protocol; IP, Internet Protocol; MIME, Multipurpose Internet Mail Extension; OSPF, Open Shortest Path First; RSVP, Resource Reser Vation Protocol; SMTP, Simple Mail Transfer Protocol; SNMP, Simple Network Management Protocol; TCP, Transmission Control Protocol; UDP, User Datagram Protocol.

provides unreliable and connectionless datagram services. IP delivers datagram from source to destination, but does not support any error-control and assistance for host and management concerns. ICMP has been developed for network layer and encapsulates the IP datagram it receives from higher layer before forwarding to the IP layer. In order to find a host or router is active, some debugging tools like Ping and Traceroute have been introduced. Ping program sets the identifier field in echo request and reply messages that are being exchanged between sender and receiver via ICMP messages. Traceroute on other hand is a UNIX program and known as Tracert in Windows identifies traces the route of a packet from a source to destination.

Internet Group Management Protocol (IGMP): IGMP protocol supports multicasting by managing group membership and works with IP at network layer. It gives the multicast routers information about the membership status of hosts or routers connected to networks.

User Datagram Protocol (UDP): The UDP uses port numbers to provide process-to-process communication and provides error and flow control at a minimum level and encapsulates and decapsulates the message. It is also known as connectionless or unreliable transport protocol. It is a very simple message-oriented protocol that uses minimum overhead and does not require any interaction between sender and receiver prior to sending any messages.

Transmission Control Protocol (TCP): It is connection oriented and a reliable protocol, also byte oriented and provides process-to-process communication using port numbers at application layer. It offers full-duplex services where the data can flow in both directions.

Stream Control Transmission Protocol (SCTP): This is a new reliable and message-oriented transport layer protocol that combines the features of UDP and TCP. It is designed to offer better services than TCP for new Internet applications such as IUA (ISDN over IP), M2UA and M3UA (telephony

signaling techniques), H248 (media gateway control), H.323 (IP telephony), and session initiated protocol (SIP) (IP telephony).

File Transfer Protocol (FTP): It is a standard technique of TCP/IP to transfer file from one host to another over Internet. The files may have different format, conventions, representation of text and data, file and directory systems, etc. FTP uses the services of TCP and client-server paradigm. It establishes two TCP connections (control connection at port 21 and data connection at port 20). It can transfer different types of files like ASCII, EBCDIC, Images.

Trivial File Transfer Protocol (TFTP): In applications where all the features offered by FTP are not needed, a modified version of FTP as TFTP has been introduced as a standard of TCP/IP. This is primarily used in the applications where we need to copy a file, for example, bootstrap and configuration files of diskless workstation or router, and so on. The TFTP software can be stored into a ROM of a diskless workstation. It uses UDP at known port 69. UDP transfers each block of data encapsulated in a separate user datagram. It is very useful for basic file transfer such as initialization of devices such as bridges, routers, etc.

Telnet: TERminal NETWORK (TELNET) is a standard TCP/IP protocol for virtual terminal service proposed by ISO and is based on popular remote-access based paradigm as client-server. It establishes a connection to a remote node where the local terminal looks like a local to remote location. It is known as general purpose client-server application program that can be used to implement a number of related applications for remote accesses. For heterogeneous systems, it offers a universal interface known as network virtual terminal (NVT) that translates data or commands from local terminal to NVT and sends to the network. It uses only TCP connection. The server uses well-known port 23 and client uses as ephemeral port. It suffers from security problems.

E-Mail: This is one of the most popular applications service over the Internet. The mail program consists of user agent (UA), message transfer agent (MTA), message access agent (MAA).

User Agent: It provides services to user for initiating a process of sending and receiving messages over Internet. It offers two classes of interfaces as command-driven (old system) and GUI-based (currently in use).

Message Transfer Agent: Client–server based MTA is responsible for providing communication for the mail. The protocol that implements MTA is known as simple mail transfer protocol (SMTP).

Web-Based Mail: Many of the websites are providing the mail services to the users such as hotmail, Yahoo, gmail, and others. The messages from sender still have to go through SMTP. The receiving side will receive the message from their web server via http.

Simple Network Management Protocol (SNMP): This protocol runs at application layer and supports different LANs, WANs that are connected by routers of different manufacturers. It consists of two components as structure of management information (SMI) and management information base (MIB). The SNMP defines the formats of the packets exchanged between a manager and agent and interprets the result and creates statistics. It reads and changes the status (values) of objects (variables) in SNMP packets.

Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP): Two protocols have been implemented based on dynamic mapping technique as ARP and RARP. ARP maps a logical address to physical while RARP maps a physical address to logical address. Both use unicast and broadcast physical addresses.

ARP expects sender asking the receiver to announce its physical address. It associates an IP address with its physical address. It can also be used over any network-like frame relay, asynchronous transfer mode (ATM), etc. Proxy ARP is a new concept for creating subnetting effect where it acts as an ARP on behalf of a set of hosts. A router running proxy ARP after receiving a request for IP address of any of the hosts sends an ARP reply giving its own physical address.

RARP provides logical address to a computer that knows its physical address. RARP request packets are broadcast while reply is a unicast. A unique set of one or more IP addresses independent of physical address may be assigned to each host and can use any of these addresses to create an IP datagram.

INTERNET PROTOCOL ADDRESSING

The IP address is a 32 bit address and is a unique address. It supports two types of addressing as class oriented and classless. Both support $2^{32} = 4,294,967,296$ addresses. The

class-oriented IP address space can be defined in five classes as A, B, C, D, and E. The first bit in all class A IP addressing is 0 while remaining 31 bits provide address space. The first two bits in all class B IP addressing are 10 while remaining 30 provide the address space. The first three bits of all class C IP addressing are 110 while remaining 29 bits provide the address space. The first four bits of all class D IP addressing are 1110 while remaining 28 bits provide address space. Finally, the first four bits of all class E IP addressing are 1111 while remaining 28 bits provide address space. Some of the materials presented can also be found in Refs. [2,5,7,8].

The IP addresses in classes A, B, and C is further divided into two sections—Netid and Hostid. Class A will have first byte (8 bit) as netid and remaining 3 bytes as hosted. Class B will have first two bytes as netid while remaining two bytes as hostid while class C will have the first three bytes as netid while remaining fourth byte as hostid. The remaining classes D and E do not have partitions.

Classes of IP Addressing

Class A is usually used by large organizations with a large number of hosts or routers attached to their networks. A large number of addresses are wasted.

Class B is usually for mid-size organizations with thousands of hosts or routers attached to their networks. Many addresses are wasted.

Class C is usually for small organizations with a small number of hosts or routers attached to their networks. The number of addresses is usually smaller than the needs of most organizations.

Class D is mainly for multicasting with address is used to define a group of hosts on the Internet.

Class E is primarily defined as a reserved address space and as such most of the addresses are wasted.

Class-oriented IP addressing schemes suffer from the wastage of addresses and also each address assignment is a multiple of a byte. The classless IP addressing offers a variable-length assignment based on masking concept and as such it avoids the wastage of address space but creates a problem in terms of assignment that is a power of 2 and must be accompanied by the mask. This class of IP addressing was introduced in 1996 and is becoming popular. Class-oriented IP addressing scheme may be considered as a part of classless IP addressing scheme.

However, the explosive growth of the Internet has led to IPv4 address exhaustion, which is estimated to enter its final stage in approximately 2011. A new protocol version, inter-networking protocol version 6 (IPv6), was developed in the mid-1990s which provides vastly larger addressing capabilities, security, and more efficient routing of Internet traffic.

IPv6 is not interoperable with IPv4. It basically creates a “parallel” version of the Internet not directly accessible with IPv4 software. This requires some kind of mapping

every networking device that needs to communicate on the IPv6 Internet. Most modern computer operating systems are already converted to operate with both versions of the IP. Currently, the Internet is facilitated by bi- or multi-lateral commercial contracts (e.g., peering agreements), and by technical specifications or protocols that describe how to exchange data over the network.

Internetworking Protocol Version 6

Internetworking Protocol Version 6 (IPv6) also known as internetworking protocol, next generation (IPng) has become standard is a modified version of IPv4 that accommodates more number of addresses. This also requires the changes in other protocols that are being used with IPv4 like ARP, RARP, ICMP, routing information protocol (RIP), and open shortest path first (OSPF). It offers the following advantages: larger address space (128 bits), better header format, support for resource allocation, support for more security, allowance for extension, and new options.

The transition from IPv4 to IPv6 is a complicated and should not include any problem. As such the Internet engineering task force (IETF) proposed three strategies to implement this transition. In the first strategy, all then hosts should have dual stack of protocols. The DNS gets a query from the host and based on it, it sends packet to appropriate protocol (IPv4 or IPv6). The next strategy uses the concept of tunneling where the IPv6 packet is encapsulated in an IPv4 packet when it enters into the region and leaves the capsule when it exits the region. Tunneling can be implemented using two mechanisms, automatic tunneling and configured tunneling. Finally, the third strategy of header translation mechanism should be used where sender and receiver do not use the same protocols and also the tunneling does not work. The header of IPv6 packet is converted to IPv4 packet. It uses mapped address to translate IPv6 to an IPv4 address.

IPSecurity

IP security known as IPsec protocol offers security at the network layer. It secures IP datagrams between two network-layer entities including routers and hosts. It finds its application in many organizations, companies, universities for creating virtual private networks (VPNs) over Internet or public networks. The corporations or universities having more sites can create their own IP network so that the data can be transmitted to these sites securely over its hosts and routers. A standalone physical network including routers, hosts, links, DNS infrastructure over the public network can be created. Such a disjoint and dedicated network is known as private network. This method of creating a private network may be expensive. Alternatively, VPN over Internet or public network can be created for transmitting traffic in an encrypted form over the Internet. The network layer provides all the types of secure properties we discussed above, for example, the confidentiality is provided by encrypting the

payload of all the datagrams before sending to the receiving node and is defined between two entities (routers, hosts, or between router and host). The encrypted payload may be any type of message, for example, TCP segment, UDP segment, ICMP, or any other message. Network layer protocol allows the receiving node to authenticate or verify the source node. The receiving node can also check the data integrity where it can determine whether data has been tampered or not during its transmission. In addition to these properties, the network layer also provides reply-back prevention where the receiving node can detect any duplicate datagram that may have been inserted by the attacker.

Domain Name System

An Internet-wide domain name system (DNS) supports the translations of IP addresses into hostnames, using a distributed database and a vast number of cooperating systems to provide the DNS name translation service.

The DNS maps the domain names of the organizations to actual IP address and as such needs coordination. It is a hierarchical system divided into separate domains. The Internet application browser forwards the domain name to the DNS server, which is normally operated by ISP, and the server locates the databases for each of the subdomains. If the domain name is www.umes.edu, the DNS server first locates the server for.edu (highest domain level); it then finds the server for UMES, the second domain, and so on. Different countries have different levels of domains. The United States usually contains three levels of domains.

The system was formerly administered by a small private company known as Network Solutions International (NSI). Looking at the exponential growth of Internet and under political pressure, the system was handed over to Internet Corporation for Assigned Names and Numbers (ICANN), which is an international non-profit organization with full responsibilities of DNS. It does not allocate domain names but defines the policies and procedures for domain name distribution and has the final say in selecting any firm for the name. The names are allocated by another organization such as VeriSign.

In order to resolve the domain names, six top level domains were introduced for Net as .com, .edu, .org, .gov, .net, and .mil. as shown below:

Education—EDU
Government—GOV
Military—MIL
International—INT
Network—NET
(Non-Profit) Organization—ORG
Commercial—COM

ICANN has introduced other top level domains as .aero (air transport companies), .coop (cooperatives), .biz (business), .museum (museums), .name (individual), .pro (professionals such as lawyers), .info (non restricted use). ICANN

is currently governed by a board of 18 members, 9 of those members are elected by the at-large membership.

The DNS was and continues to be a major element of the Internet architecture, which contributes to its scalability connectivity for heterogeneous systems. It also contributes to controversy over trademarks and general rules for the creation and use of domain names, creation of new top-level domains and the like. These developments are taking place in parallel with the more traditional means of managing Internet resources. They offer an alternative to the existing DNS with enhanced functionality.

Dynamic Domain Name System

The DNS maintains a DNS master file which needs to be updated manually for any changes like adding a new host, changing IP address, removing host or others. In order to maintain the DNS master file automatically, dynamic domain name system (DDNS) technique has been introduced. The binding between name and address information is sent usually by DHCP to a primary DNS server which in turn updates the file based on zones. It uses authentication mechanism against any attack.

ROUTING PROTOCOLS

Unicast Communications

Internet is very big and is being partitioned into autonomous systems (ASs). An AS is a group of networks and routers under the control of a single administration. Routing within an AS is known as intradomain routing. Routing between ASs is known as interdomain routing. For details, please refer to Refs. [2,3,6,7,11,12].

Routing Information Protocol (RIP): RIP is an intradomain routing protocol used inside an AS. It is based on distance vector routing where it calculates the least cost route between any two nodes with minimum distance.

Open Shortest Path First (OSPF): It is intradomain routing protocol based on link state routing and works an AS. Each node in the domain has the information about the topology of the domain including list of nodes, links, their connections, type, costs, and the conditions of the links. The node uses Dijkstra's algorithm to build a routing table.

Border Gateway Protocol (BGP): It is an interdomain protocol based on path vector routing technique. It is derived from the distance vector routing with minor differences. Here, one or more nodes can be declared as a representative of the entire AS. It creates a routing table and informs the representative nodes of all neighboring ASs.

Multicasting Communication

Unicasting provides one-to-one communication and the router forwards the message through one of its interfaces.

Multicasting provides one-to-many communication where the same message is sent to all nodes of a selected group at the same time. Broadcasting provides one-to-all where the same message is sent to all the connected nodes in the network. Multicast protocol finds its applications in access to distributed databases, information dissemination, dissemination of news, teleconferencing, distance learning, etc.

Multicast Open Shortest Path First (MOSPF): It is an extension of the OSPF and uses multicast link state routing for generating source-based routes. It is a data-driven protocol where the router generates the Dijkstra's shortest path tree after receiving the datagram with associated source and destination nodes.

Core-Based Tree (CBT): It is a group-shared protocol that uses core as a root of the tree. Each AS is partitioned into regions and a core (center router) is chose for each region. Here, the source sends multicast packet to core router in encapsulated format of unicast. The core router decapsulates the packet and forwards it to all the interested interfaces.

Multicast Backbone (MBONE): A small number of routers with multicast capability are present in Internet and as such multimedia and real-time communication cannot take place efficiently over the Internet. The concept of tunneling has been used to support this kind of communication in MBONE protocol.

Resource-Reservation Protocol (RSVP): A user uses RSVP to make request for a specific *quality-of-service* (QoS) from the network for his/her application. The RSVP carries the request through the network, visiting each node the network uses to carry the stream. At each node, RSVP attempts to make a resource reservation for the application stream. It consist of two modules as admission and policy. The admission module determines whether the node has sufficient available resources to supply the requested QoS while the policy module determines whether the user has administrative permission to make the reservation. If either check fails, the RSVP program returns an error notification to the application process that originated the request. If both checks succeed, the RSVP sets parameters in a *packet classifier* and *packet scheduler* to obtain the desired QoS.

A primary feature of RSVP is its scalability. RSVP scales to very large multicast groups because it uses receiver-oriented reservation requests that merge as they progress up the multicast tree. While the RSVP protocol is designed specifically for multicast applications, it may also make unicast reservations. RSVP runs over IP, both IPv4 and IPv6.

REAL-TIME INTERACTIVE SERVICES OVER INTERNET

Audio and video services over Internet can be implemented in three different ways: streaming stored audio/video, streaming live audio/video, and interactive audio/video.

In streaming stored audio/video, the compressed files are available on a web server. A client (using HTTP and GET commands) downloads these files as a text file over the Internet, for example, song files, books on tapes, lecture notes, video movies, TV shows, music video clips, video lectures and presentations, etc. In some books, this service is also known as on-demand audio/video. The larger files even after compression may cause a problem in the sense that they cannot play until the entire file is downloaded. The file can also be downloaded from the web server using media player. The web server stores two different files as audio and video and a metafile (information about audio and video files). A protocol known as real-time streaming protocol has been proposed that works with media server and offers more functionalities in streaming process.

In interactive audio/video, the users can access interactive communication over the Internet for example, VoIP or Internet telephony (e.g., gtalk), and Internet conferencing. A *real-time transport protocol* (RTP) has been introduced to handle real-time traffic over the Internet. It is used with UDP. It works between application and UDP layers. It supports one type of message between sender and receiver. Another modified version of RTP known as *real-time transport control protocol* handles more messages between sender and receiver that can offer a better quality and flow of data. The VoIP or Internet telephony allows the users to use the Internet (packet switched networks as opposed to circuit-switched telephone networks). The communication between server and receiver makes use of two protocols as SIP (defined by IETF) and H.323 (defined by ITU).

Protocols for Real-Time Interactive Applications

Real-Time Transport Protocol (RTP): This protocol is defined in request for comment (RFC) 3550 that supports the transportation of real-time applications in the formats of PCM (pulse-coded modulation), GSM (global system for mobile communication), and MP3 for sound and MPEG and H.263 for video. It can also be used to transport proprietary sound and video formats.

Session Initiated Protocol (SIP): It is defined in RFC 3261 and RFC 5411 is a lightweight protocol that establishes communication between sender and receiver over IP network, allows the sender to determine the current IP address of receiver and communication management like change of encoding, including new participants, call transfer, call holding, and others. This is primarily used in video conference calls and also text sessions over Internet and actually has become very popular in instant message applications. It allows the users to communicate with phone attached to circuit-switched telephone networks. It addresses only session initiation and management and can work with RTP or with other standard speech and video codecs. It was defined by IETF and is based on the concepts of web, DNS, and Internet e-mail.

INTERNET SERVICE PROVIDERS

Internet is not a simple hierarchical structure but is interconnection of a number of wide area and LANs that are joined by switching nodes and internetworking devices. Internet service providers (ISPs) companies started in 1995 to provide Internet access to the users. There are international, national, regional, and local service providers. At the top level of structure, international service providers connect countries together. The national service providers are the backbone networks that provide connectivity to the users within country. Some of national service providers in North America include: SprintLink, PSINet, UUNet Technology, AGIS, and Internet MCI. These networks are connected by switching nodes that are usually maintained by third parties known as network access points and offers data rates of 600Mbps. The regional service providers are connected to one of the national service providers. The local service providers at the lowest level provide direct service to the users and are connected either to regional or national service providers.

The Internet discussed above is also known as a public Internet. There are also many private networks, such as certain corporate and government networks, whose hosts are not accessible (i.e., they cannot exchange messages with) from hosts outside of that private network. These private networks are often referred to as intranets, as they often use the same "Internet technology" (e.g., the same types of host, routers, links, protocols, and standards) as the public Internet.

The Internet supports two types of services to its distributed applications: a *connection-oriented* service and a *connectionless* service. In connection-oriented service, the Internet guarantees that data transmitted from a sender to a receiver will eventually be delivered to the receiver in-order and in its entirety. In contrast, in connectionless service, Internet does not make any guarantees about eventual delivery. Typically, a distributed application makes use of one or the other of these two services and not both. Currently the Internet does not provide a service that indicates *how long* it will take to deliver the data from sender to receiver. And except for increasing your access bit rate to your ISP, you currently cannot obtain better service by paying more.

Today, the Internet is an interconnected network of networks comprised of approximately 150 million hosts worldwide (Internet Software Consortium at <http://www.isc.or>). The number of computer security incidents handled by the CERT Coordination Center (CERT/CC) has grown from 6 in 1988 to 52,658 in 2001. By the end of September 2002, the CERT/CC had already seen over 73,000 incidents [15], and yet, despite serious security shortcomings, TCP/IP is still the standard protocol suite for network communications on the Internet, greatly limiting our ability to track and trace Internet cyber attacks to their source. Some of the information presented here is derived from Refs. [2,3,5–8].

INTERNET STANDARDIZATION

At the technical and developmental level, the Internet is made possible through creation, testing, and implementation of *Internet standards* and also known as *cyber standards*. These international standards are developed by the IETF and the World Wide Web Consortium. The IETF standards documents are called RFCs. The discussions, results, and final standards are published in a series of publications known as RFC that is freely available on the IETF website. New technologies and methods of networking for Internet are included in RFCs that constitute Internet standards.

A typical Internet infrastructure consists of hardware and a system of software layers that manages various aspects of Internet architecture for proper communication and deployment of various applications. The standardization and other responsibilities of architectural design aspect of Internet are delegated to IETF. There are other standards organizations that are involved in standards, data communication in North America and work closely with various standards committees, forums, and government regulatory agencies.

Standards Organizations, Forums, and Regulating Agencies

1. *International Standards Organizations (ISO)*: Voluntary organization for worldwide agreement on international standards and its organization chart is shown in Figure 30.4.
2. *International Telecommunications Union-Telecommunications Standards Sector (ITU-T)*: United Nation formed this committee as a part of its International Telecommunication Union.

3. *American National Standards Institute (ANSI)*: A private, non-profit corporation, serves as national coordinating institute for voluntary standardization in the United States.
4. *Institute of Electrical and Electronics Engineers (IEEE)*: Largest professional engineering society in the world. Its aim is to advance theory, creativity, and product quality in field of stated engineering disciplines.
5. *Electronic Industries Association (EIA)*: Aligned with ANSI, EIA is a non-profit organization responsible for electronic manufacturing products.

Forums

1. *Frame Relay Forum*: formed by Digital Equipment Corporations, Northern Telecom, Cisco, and StratCom to promote the acceptance and implementation of Frame Relay.
2. *ATM Forum*: promotes the acceptance and implementation of ATM technology.

Regulatory Agencies

1. *Federal Communications Commission (FCC)*: has authority over interstate and international commerce as it relates to communications.
2. *Internet Society (ISOC)*: International non-profit organization for providing support for Internet standards.
3. *Internet Architecture Board (IAB)*: Technical advisor to ISOC.
4. *Internet Engineering Task Force (IETF)*: Forum of working groups, managed by the Internet Engineering Steering Group (IESG).

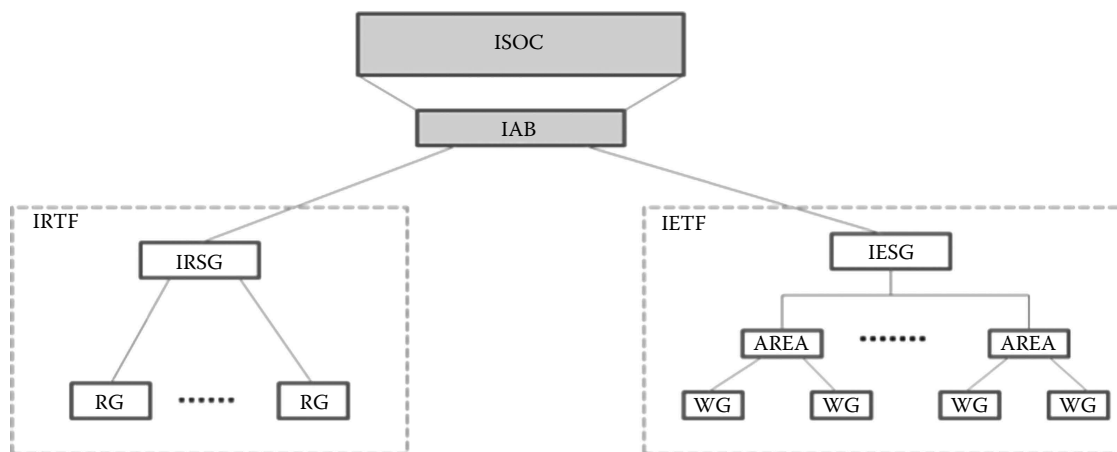


FIG. 30.4

Internet Standards Organization chart. ISOC, Internet Society; IAB, Internet Architecture Board; IRTF, Internet Research Task Force; IRSG, Internet Research Steering Group; IETF, Internet Engineering Task Force; IESG, Internet Engineering Steering Group; WG, Working Group.

5. *Internet Research Task Force (IRTF)*: Forum of working groups managed by Internet Research Steering Group (IRSG).
6. *Internet Assigned Number Authority (IANA) and Internet Corporation for Assigned Names and Numbers (ICANN)*: IANA supported by the United States was responsible for Internet Domain names and addresses. ICANN is a private non-profit organization.
7. *Network Information Center (NIC)*: Responsible for collecting and distributing information about TCP/IP protocols.

CYBER SECURITY AND SECURITY MANAGEMENT

The creation and phenomenal growth of the Internet has spawned the emergence of a global information society. Businesses possessing highly distributed information assets can share information internationally easily, efficiently, quickly, and seamlessly among their divisions, partners, suppliers, and customers. Government also uses the Internet to provide information and services to their citizens and to the world at large. Governmental use of the Internet will increasingly extend to international information sharing and collaboration. The scientific, engineering, and educational communities are all using the Internet as an indispensable tool for collaboration and rapid dissemination of information on advances in research and practice at all levels of scientific and engineering endeavor.

Cyber attack is defined as a crime that occurs either in a computer or network of organizations, companies, or any other corporation. The intention of a successful hacker involved in a cyber attack is to gain the access of the victim's computing assets (processors, memory, etc.), and gather sensitive internal data, victim's database servers containing confidential documents, cause disruption, monitor on-line activities, access to instant message and e-mail accounts, and denial of service in some cases. Increasingly, the results of cyber attacks can be felt in a tangible world—victims of such attacks typically suffer financial losses and might also lose credibility. Some of the materials presented here have been derived from Refs. [1–9,13–19].

All of the benefits that the Internet and the global information society can provide, including support for the most basic and essential services that government provides, are subject to disruption by Internet-based cyber attacks. Historically, attacks on a nation's essential services typically required a physical attack that crossed the nation's borders slowly enough that it was subject to recognition and interception by that nation's military. At the very least, some physical evidence would likely be left that would allow for the tracking, tracing, and identification of the perpetrators and the tools or weapons used in the attack. Today, cyber attackers use the speed and global connectivity of the Internet to make national boundaries irrelevant, and sophisticated attackers

leave little in the way of electronic evidence that can be used to track or trace them.

Perhaps the greatest threat to the Internet today is the abysmal state of security of so many of the systems connected to it. There are many contributing factors, including commercial off-the-shelf (COTS) software, in which the number of features and rapid time to market outweigh a thoughtful security design. New vulnerabilities are continually being discovered in such software. The widespread use of many COTS products means that once a vulnerability is discovered, it can be exploited by attackers who target many of the thousands or even millions of systems that have the vulnerable product installed. A lack of security expertise by most Internet users means that vendor security patches to remove the vulnerabilities will not be applied promptly, if at all. As a result, systems with unpatched vulnerabilities can be easily compromised, in large numbers, by motivated attackers, who will then use these systems as launching points to concentrate an attack against better-protected systems and to hide the tracks of the attacker.

Society continues to migrate increasingly critical applications and infrastructures onto the Internet, despite severe shortcomings in computer and network security and serious deficiencies in the design of the Internet itself. Today's Internet environment supports a global, less trustworthy user population, but provides a broad range of social, legal, economic, political, and infrastructural services, and hence offers far more motivation for malicious cyber attacks. Accountability for cyber attacks that cause serious damage is essential. The ability to accurately and precisely assign responsibility for cyber attacks to entities or individuals (or to interrupt attacks in progress) would allow society's legal, political, and economic mechanisms to work both domestically and internationally, to deter future attacks and motivate evolutionary improvements in relevant laws, treaties, policies, and engineering technology.

Basically, if one is connected to networking and is using it for any application, you are available to everyone else on the network. As economies around the globe become more dependent on information, networking and communications technology, they are becoming more vulnerable to network attacks (e.g., threats to the Internet, as well as other private and public networks). The most serious cyber security risks are those that threaten the functioning of critical information infrastructures such as financial services, control systems for utilities, gas, drinking water, and other utilities; transportation, airport, and air traffic control systems; logistics systems; and government services [6,10,11,13,14,16,19].

Cyber Attack Tools and Well-Known Attacks

The tools available for these types of attacks include: password guessing, self-replicating code, password cracking, exploiting known, vulnerabilities, disabling audits, back

doors, hijacking, sessions, sweepers, sniffers, packet spoofing, GUI automated probes/scans, denial of service, www attacks, stealth/advanced scanning techniques, burglaries, network management diagnostics, distributed attack tools (such as distributed denial of service, DDoS), cross-site scripting sophisticated command and control and many others. Some of the known attacks and measures to protect computing resources are described below. Some of the material presented below has been derived from [6,10,11,13,14,16,19].

Remote Login: attacker getting access to your computer will be able to view or access the files to actually running programs on the computer.

Application Backdoors: Some programs have special features that allow for remote access. Others contain bugs that provide a backdoor or hidden access that provides some level of control of the program.

SMTP Session Hijacking: SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (Spam) to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.

Operating System Bugs: Like applications, some operating systems have backdoors. Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.

Macros: To simplify complicated procedures, many applications allow you to create a script of commands that can be used frequently to run the application. This script is known as a macro. Hackers/intruders can create their own macros that can destroy the data and also crash the computer.

Spam: It is electronic equivalent of junk mail and usually harmless but always annoying. Spam can be dangerous as it contains links to websites. Clicking on these, you may accidentally accept a cookie that provides a backdoor to your computer.

Redirect Bombs: Hackers can use ICMP to change or redirect the path information by sending it to a different router. This is one of the ways that a denial of service attack is set up.

Source Routing: In most cases, the router determine the path for packets over Internet. But the source routing provides packets that can arbitrarily specify the route for the packet. Hackers take the advantage of this route to make the packets appear to come from a trusted source or even from inside the network. Most firewall products disable source routing by default.

E-Mail Attack: The most straightforward and effective way for an attacker to launch his own code on his victim's computer is to actually attach his executable to an e-mail message. The most common of this kind of attack is known as

"Mass Mailing Worms," like the Nimda worm, which made rounds back in 2001, or the more recent variants of Bagle and Netsky worms, which made up a substantial part of the e-mail traffic during 2005.

In July 2005, the United States Computer Emergency Readiness Team issued an advisory that suggested that attackers were sending out e-mail attachments with Trojan files, which when launched, are able to perform the following functions:

- Collection of usernames and passwords for e-mail accounts
- Collection of critical system information and scanning of network drives
- Use of infected machine to compromise other machines and networks
- Downloading of further programs (e.g., worms, more advanced Trojans)
- Uploading of documents and data to a remote computer

Network Attack: When an attacker decides to target a specific corporation, they can either get personal with the employees by making use of e-mail and other similar technology, or go through the gateway. Finding the location (IP address) of the company network is usually quite straightforward, since a lot of organizations host the e-mail server on the company network. Even if it is not the case, e-mail headers of mail sent out by employees, usually contain enough information to point toward the internal and external IP address of the network. From there, the attacker will enumerate the IP address pool belonging to (or hired by) the victim, and enumerate the services exposed to the Internet, such as SMTP, HTTP, or VPN.

Instant Messenger Attacks: Instant messenger (IM) attacks are very similar to e-mail. With IM, the attacker is able to more easily and instantly communicate with his/her victim. However, most IMs have the following security differences from e-mail: it initially requires more effort to get the victim to trust because (with MSN and Yahoo Messenger), one is required to sign up. The victim can choose whom to communicate with and therefore (unlike e-mail), can choose to "not talk to strangers." However, when those steps are followed, it becomes easier for the attacker to get his own custom code on the victim's computer, or gain access to sensitive information. What makes instant messaging easier is that unlike e-mail, IM is not constantly targeted by opportunistic attacks and therefore most people will trust content coming from their IM when they would not give the same content coming from e-mail a second thought. Targeted attacks via IM are becoming more popular in business arena due to faster transmission and arrival of the messages than e-mail.

Denial of Service: Attacker or intruder or hacker sends a request from his/her machine to the server for connection. When the server responds with an acknowledgement and tries to establish a session with that machine, it cannot find the system that made the request. By inundating a server

with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash thus causing a denial of service. This is particular very bad for Internet-based users as the website is unable to provide any service.

Distributed Denial of Service (DDoS) Attacks: DDoS allow attackers to block website of the victim rather than steal information. DDoS attacks typically consist of flooding the network with packets, reaching its limits. As a result, legitimate requests are lost or at least the service becomes too slow to work with. The attackers gather a large botnet, as described below, by making use of opportunistic attacks. Then they use these botnets to direct thousands of systems to attack a single server or network. Even when a service, such as eBay, has much larger bandwidth than any of the bots, it is no match against all of them at the same time.

Buffer Overflow Attacks: A buffer overflow is an attack that could be used by a hacker to get full-system access through various methods. It is similar to “Brute Forcing” a computer in that it sends an immense attack to the victim computer until it cracks. Most Internet security solutions today lack sufficient protection against these types of attacks.

Cyberbullying: Cyberbullying is type of cyber attack that harasses, or bullies someone over Internet. Other forms of bullies have been widely used include physical intimidation, postal mail, or the telephone. Now, with the developments of a number of applications over Internet, this has been used in e-mails, instant messaging, web pages, and digital photos and computers, cell phones, and PDAs are new tools that can be applied for these activities.

Malicious Code Insertion: An attacker may be able to insert malicious code into any file, including common file types that we usually consider safe. These files may include documents created with word processing software, spreadsheets, or image files. After corrupting the file, an attacker may distribute it through e-mail or post it to a website.

There are various types of malicious code, including viruses, worms, and Trojan horses. However, the range of consequences varies even within these categories. The malicious code may be designed to perform one or more functions, including

- Interfering with computer’s ability to process information by consuming memory or bandwidth (causing your computer to become significantly slower or even “freeze”)
- Installing, altering, or deleting files
- Giving the attacker access to your computer

Hidden Threats

Some apparently useful programs also contain features with hidden malicious intent. Such programs are known as Malware, Viruses, Trojans, Worms, Spyware, and Bots.

Malware is the most general name for any malicious software designed, for example, to infiltrate, spy on, or damage a computer or other programmable device or system of sufficient complexity, such as a home or office computer system, network, mobile phone, automated devices, or robots.

Viruses are programs which are able to replicate their structure or effect by integrating themselves or references to themselves, etc. into existing files or structures on a penetrated computer. They usually also have a malicious or humorous payload designed to threaten or modify the actions or data of the host device or system without consent. For example, by deleting, corrupting, or otherwise hiding information from its owner.

Trojans (Trojan Horses) are programs which may pretend to do one thing, but in reality steal information, alter it, or cause other problems in a computer or programmable device/system. Trojans can be hard to detect.

Spyware includes programs that surreptitiously monitor keystrokes, or other activity on a computer system and report that information to others without consent.

Worms are programs that are able to replicate themselves over a (possibly extensive) computer network, and also perform malicious acts that may ultimately affect a whole society/economy.

Rootkit: A piece of software that can be installed and hidden on a computer without the user’s knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of an vulnerability or has convinced you to download it. Rootkits do not represent malicious code, but they hide malicious code within given application/software. Attackers can access information, monitor your actions, modify programs, or perform other functions without being detected.

Bots are programs that take over and use the resources of a computer system over a network without consent, and communicate those results to others who may control the Bots. An attacker usually gains control by infecting the computers with a virus or other malicious code that gives the attacker access. Your computer may be part of a botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing spam and viruses to conducting denial-of-service attacks.

Antivirus programs and Internet security programs are useful in protecting a computer or programmable device/system from malware. Such programs are used to detect and usually eliminate viruses. Care should be taken in selecting anti-virus software, as some programs are not as effective as others in finding and eliminating viruses or malware. Also, when downloading anti-virus software from the Internet, one should be cautious as some websites say they are providing protection from viruses with their software, but are really trying to install malware on your computer by disguising it as something else.

As an alternative, some vendors are developing products and tools that may remove a rootkit from a computer. If the software cannot locate and remove the infection, operating

system may have to be reinstalled with the system restore disk supplied with the computer. Note that reinstalling or restoring the operating system typically erases all the other files. Also, the infection may be located at such a deep level that it cannot be removed by simply reinstalling or restoring the operating system.

Debilitating worms and computer viruses have caused a lot of destruction on the computer resources for a number of years, as evidenced by the damage caused by such programs as Sasser, Blaster, Netsky, Welchia, and Code Red [6,13,14].

Phishing and Pharming

The booming growth of Internet-services and growth has given opportunities to the attackers for attacking financial institutions in terms of significant losses through “phishing” and “pharming” operations (for information on trends and counter-measures to combat phishing and pharming, visit the website of the Anti-Phishing Working Group, an industry association in California [20]).

Phishing is the act of sending an e-mail that claims to be from an established legitimate enterprise in an attempt to scam a user into surrendering private information for the purposes of identity theft. *Pharming* seeks to obtain personal or private (usually finance related) information by creating false websites (domain spoofing). More information on phishing and pharming can be found in Chapter 31 of this book.

Targeted Cyber Attacks

A targeted attack is much more effective and damaging for the victim since the actions performed by the malicious hacker are tailored. This means that it is much more difficult to stop a targeted attack than an opportunistic one simply because the attacks themselves are not general. E-mail is of course a medium that is used to carry out both opportunistic and targeted attacks. Most security solutions handle general attacks quite well, because the security solutions themselves are for the general public. An e-mail content filtering solution that catches e-mail worms by identifying them through a signature aimed toward known worms will most likely let through malicious executable code, which is targeted for a specific company running. Some of the concepts and salient features of attacks and measures are derived from Ref. [6].

SECURITY CONCERNS

Security concerns are in some ways peripheral to normal business working, but serve to highlight just how important it is that business users feel confident when using IT systems. Security will probably always be high on the IT agenda simply because cyber criminals know that a successful attack is very profitable. This means they will always strive to find new ways to circumvent IT security, and users will consequently

need to be continually vigilant. Whenever decisions need to be made about how to enhance a system, security will need to be held uppermost among its requirements. Some of the material discussed here has been derived from Ref. [8].

Most attacks on the Internet consist of opportunistic attacks rather than attacks targeted for some specific entity. An opportunistic attack is when an attacker targets various different parties by using one or various generic ways to attack such parties, in the hope that some of them will be vulnerable to attack. In an opportunistic attack, an attacker will have a large number of targets and will not care that much on who the victim is, but rather on how many victims there are. Examples of opportunistic attacks: 419 scams, mass mailing worms, trojans e-mailed to various people, scams involving well-known services such as PayPal or Ebay, mass scanning for vulnerable services (SSH, UPnP, IIS servers, etc.), and many others. Numerous tests and surveys have concluded that on average, it takes about 4 min for a new Windows machine exposed to the Internet to get hacked. On the other hand, various individual organizations are still potential victims to targeted attacks. Some of the motivations behind such attacks include: industrial espionage, publicity attacks, malicious insider, personal attacks, and others. Some of the material presented here is being derived from Refs. [12,13,17].

CYBER SECURITY MANAGEMENT

The secured communication mechanism over Internet for any applications must have the following properties:

Confidentiality: The contents of the message should be known to only sender and receiver when communicating over the Internet. Encryption has been used to provide this property for secured communication over the Internet.

End-point authentication: The sender and receiver communicating over Internet should be able to identify each other.

Message integrity: Even if sender and receiver are able to authenticate each other, the contents of the message should not be changed during communication.

Operational security: The attackers can access the networks of the organizations, companies, universities that are connected to Internet.

Any application running at application layer using the protocol gets security services like confidentiality, authentication, or integrity. Under the application layer, each layer is also using security in its respective protocols. As such application enjoys the security offered by these layers, that is, transport, network, and link.

Measures against Cyber Attacks

This section presents a list of measures that can prevent our resources against the attacks:

- Limiting the posting of personal information on the net
- Documenting the activities—by keeping records of any online activities
- Report cyberbullying to the appropriate authorities
- Practicing good online habits
- Using and maintaining anti-virus software
- Exercising caution with e-mail attachments
- Avoiding downloadable files on websites
- Keeping the software up to date
- Maintaining security settings
- Installing and maintaining a firewall

There exist a number of configurations for making customized firewalls that allows addition and removal of filters based on several conditions. They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer. They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways. They rely on algorithms to recognize and process application layer data instead of running application specific proxies. Stateful multilayer inspection firewalls offer a high level of security, good performance, and transparency to end users. They are expensive however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel. Some of the known configurations include: IP addresses, domain names, protocols, IP, TCP, HTTP, FTP, UDP, ICMP, SMTP, SNMP, Telnet.

An organization can also use one or two dedicated machines to handle a specific protocol and block that protocol on all other machines. Following are some of the configurations that can be used to implement this:

Ports: The server machine is running a web (HTTP) server and FTP server, the web server would typically be available on port 80, and the FTP server would be available on port 21. An organization can block port 21 accesses on all machines except one server within the organization.

Specific Words and Phrases: The firewall will sniff (search through) each packet of information for an exact match of the text listed in the filter. For example, we can configure the firewall to block any packet with word or phrases. We can include as many words, phrases, and variations of them as needed.

A software firewall can be installed on the computer in our home that has an Internet connection. This computer is considered a *gateway* because it provides the only point of access between our network and the Internet. The firewall offers a variety of features that can be used to protect applications from hackers. These include: authentication, computational efficiency, communication, real-time involvement, nature of trust requirements (local network and external networks), nature of security guaranty, storage of policies and can be used to configure the firewall depending on the applications.

Network Infrastructure for Cyber Security

The function of network framework for a cyber infrastructure is to provide a platform for understanding the dynamics of potential cyber-security issues and provide a possible integration of various entities for a possible solution to the problem. The cyber security is very complex problem and as such the framework has to describe a number of inter-related and interleaved accurately and precisely. The following is a list of functions that the framework for cyber infrastructure should possess to provide protection against cyber attacks:

- Develop mechanisms to respond to cyber incidents leading to cyber attack
- Develop effective tools of counter measures against cyber attacks
- Assess effect of potential cyber threats/attacks on computing and network infrastructures
- Assess the vulnerabilities of critical information infrastructures
- Improve information security risk management mechanisms in the public and private sectors
- Improve risk management and threat assessment
- Improve information exchange and sharing within and between key stakeholders in public and private sector entities for critical decision policy
- Improve regulatory tools and mechanisms to minimize cyber risks and protect resources
- Develop effective law enforcement tools to analyze hacking incidents and systems (network forensics), as well as to impose penalties and sanctions
- Improve the security of system and various application software running
- Conduct outreach to all key stakeholders with a view to make appropriate decisions
- Prevent debilitating damage to critical information infrastructures and minimize the risk of cyber attacks
- Organize effective international coordination among public- and private-sector entities
- Monitor the performance of cyber-security initiatives

A brief discussion of the most important of these functions is next. Some of the material presented here is derived from Refs. [3,4,6,8,9–12,14–16,19,20].

Use of Network Framework for Cyber Security

The network framework is based on three entities of stakeholders (policymakers, policy implementers, and operational personnel), which exchange three types of information on cyber security: assessments, responses, and policy. Information exchange occurs both among the entities and between individual entities and their peers in outside organizations at all levels. The framework provides communications across all the entities at all levels.

At a lower level, various involved within the organizations should have a policy to handle cyber security. At the second level, it requires information exchange between stakeholders at different levels in the same organization and with other organizations regarding threats that have been encountered and handled. At the third level, procedures for handling such incidents are required and, at the fourth level, legal or law enforcement sanctions may need to be applied. At a higher level, that is, national, the major network entities are central coordinating bodies, telecommunications regulators and e-economy ministries, intelligence agencies, law enforcement bodies, and national and governmental CERTs and information sharing and analysis centers (ISACs). CERTs are teams of ICT professionals who prepare for, and respond to, cyber incidents. Typically, they are created within an organization to serve its specific cyber-security needs.

An ISAC is a body that allows multiple organizations within a given sector to exchange information. ISACs can belong to the private sector and communicate with the public sector. Governments also establish ISACs. The U.S. Department of Homeland Security, for example, has established several ISACs to facilitate information sharing and network protection in critical infrastructure sectors [4,8,9,16].

At the highest level, the framework supports the communication for multinational firms, political and military alliances, which coordinate with such international bodies as the ITU, G8, and the United Nations and its specialized agencies. The implementation of framework at this international level includes individual national ministries (telecommunications, intelligence, e-economy, and defense ministries, together with law enforcement bodies) and the operational level of national firms (including software and hardware vendors), CERTs, and national defense organizations.

The following section describes various security mechanisms that have been used in various applications.

SECURITY MEASURES FOR NETWORK INFRASTRUCTURE

Preventing network attacks will also prevent other tasks that might follow. However, it is generally accepted that security is a process, not a product.

Reducing the Surface Area: A simple system will therefore have less chance of falling prey to attacks, simply because there is exposure to attack. Understanding how a security system works means that one can also understand where a security system fails. When a security system is simple, it is easy to close its security flaws. On the other hand, when a security system is complex, the security designer and the attacker will keep on finding new flaws in the system forever.

Adequate Protection: Most modern networks are equipped with various security solutions to prevent against the majority of common Internet attacks. These solutions usually cope

quite well with the majority of opportunistic attacks such as worms and so on, but how do they cope with the determined, financially backed up attackers?

Firewall: As described earlier, traditional security measures such as firewalls can be circumvented quite easily. The firewall is in fact a very good security solution especially at covering up vulnerable services that should never be exposed to aggressive networks such as the Internet. It means that the firewall is limited to protecting against a good number of opportunistic attacks as well as limiting scope for attack for the determined attacker. Having a well-configured firewall minimizes exposure and allows the administrator to focus on securing more sensitive or vulnerable parts of the network. It possesses a number of properties such as authentication, computational efficiency, communication, real-time involvement, nature of trust requirements (local network and external networks), nature of security guaranty, and storage of policies.

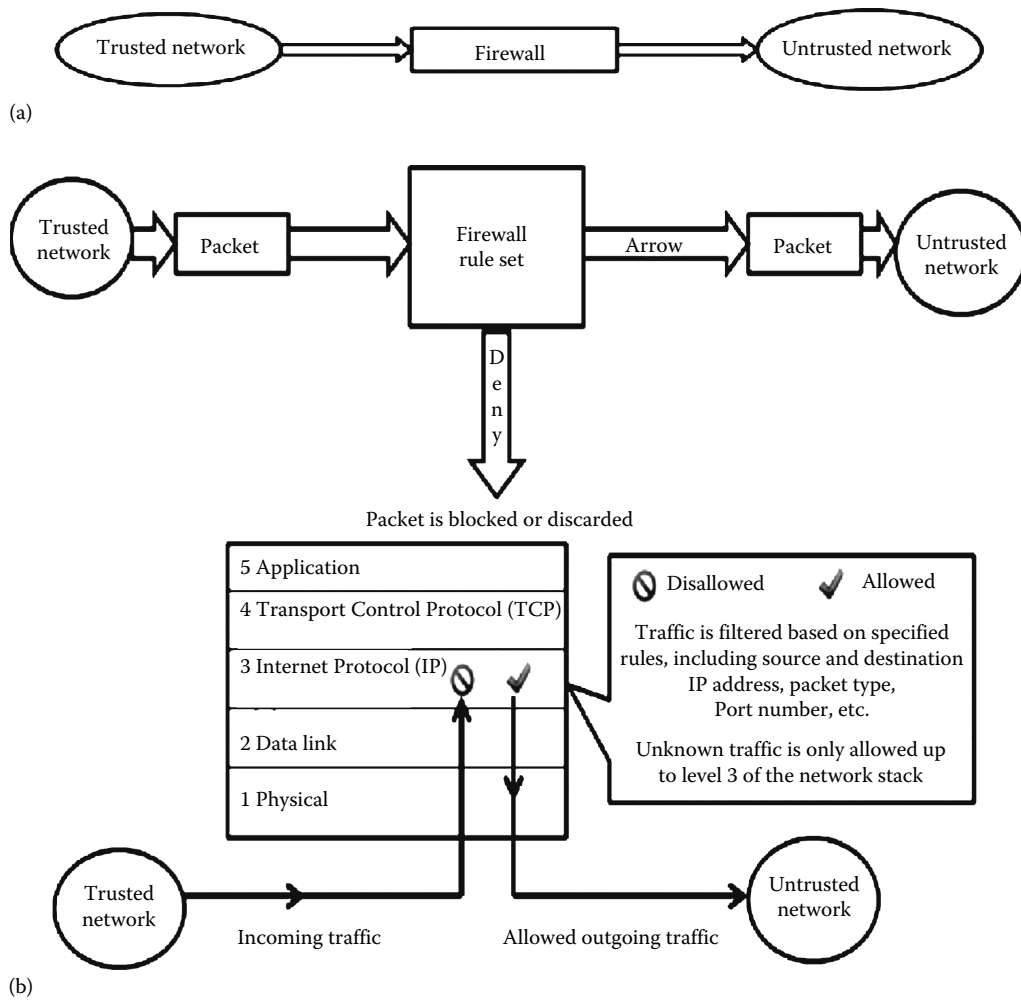
The basic concept of firewall is shown in [Figure 30.5a](#) and [b](#). There are two access denial methodologies used by firewalls. It may allow traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. The type of criteria used to determine whether traffic should be allowed through varies from one type of the firewall to another. Firewalls may be concerned with the type of traffic, or with source or destination addresses and ports. They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through.

Firewalls can operate into two broad categories:

1. Packet filters
2. Application level gateways

Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router. A router is a device that receives packets from one network and forwards them to another network. In a packet-filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. Rules can include source and destination IP address, source and destination port numbers, and protocol used. The advantage of packet-filtering firewalls is their low cost and low impact on network performance. Most routers support packet filtering. Even if other firewalls are used, implementing packet filtering at the router level affords an initial degree of security at a low network layer. This type of firewall only works at the network layer and as such does not support sophisticated rule-based models like network address translation routers that can hide the IP addresses of computers behind the firewall, and offer a level of circuit-based filtering.

Application level gateways, also called proxies, are application specific firewall category. They operate at application

**FIG. 30.5**

(a) Basic principles of Firewall. (b) Operational Firewall.

layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will not allow any ftp, web access, e-mail, telnet, or other traffic through. Because they examine packets at application layer, they can filter application specific commands such as *http:post* and *get*, etc. This cannot be accomplished with either packet filtering firewalls or circuit level neither of which knows anything about the application level information. Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance.

Content Filtering: Content filtering can play a major role in protecting organizations and ISP customers against targeted attacks. A content filtering solution for e-mail, which goes beyond scanning attachments using an anti-virus, can help administrators detect and possibly block an attack from a competitor. For example, some content-filtering solutions can rate executables according to their functionality. Instead of just matching executable content against a list of signatures,

such software is able to identify functions that could be attributed to malicious behavior and blocks. This adds an extra layer of protection against one way to bypass anti-virus. That alone is not enough, and some products also catch known exploits that bypass anti-virus software, but somehow allow access attackers to get on a victim's computer. As one can see, such products try to cover whatever conventional products do not cover—and some of these attacks are ones that a targeting intruder is going to make use of.

Intrusion Prevention Systems: Intrusion prevention systems allow administrators to detect and block attacks reactively. Although these systems do not prevent attacks, they do actually stop attacks from successfully exploiting vulnerabilities. There are various forms of intrusion prevention systems—network based such as Snort inline as well as host based such as Microsoft's DEP introduced with Windows 2003 and XP SP2 [1]. One problem with intrusion prevention systems is that they have a tendency to give false positives and therefore blocking legitimate activity. Similar to other security measures, they need to be fine-tuned for the particular environment needed.

Penetration Testing and Security Auditing

One way to actively test the security of a computer or network system is to do what the attacker is supposed to do in a legitimate way, that is, perform a penetration test. These tests, performed by professionals will usually yield the following results: proof that the computer or network system can be hacked. A professional will almost always be able to successfully attack a client's system provided that it is functional and complex enough. This of course depends on the amount of time given to the professional and also the amount of experience and knowledge the professional has, identify one or maybe a few easy targets in the system, which allow the penetration tester (and also the attacker) to successfully attack a system.

Penetration testing is very good for simulating a targeted attack. Even though a penetration test is usually very useful, especially in proving to the higher management that the network can in fact be attacked, it does not provide the same results that a complete security audit does.

Penetration testing allows a professional to look at the system from an attacker's perspective—from outside and exploiting just one vulnerability in a critical system is usually enough to gain access. This means that from this perspective, it is very difficult to identify all security weaknesses in a system. On the other hand, a security audit allows one to identify weaknesses in the system itself from a designer's point of view. Such an approach should give a more thorough analysis of the system and therefore allow the security auditor to identify theoretical and practical weaknesses that the penetration testing approach does not necessarily identify. A security audit also analyzes any security policy that the organization might have.

Good security policies are very important not only when a security incident occurs, but also when preventing an attack in the first place. A security audit may involve auditing any source code—especially home-grown applications. This will allow the discovery of any developer errors that might result in security bugs. It might also uncover intentional or unintentional backdoors in the software itself, auditing of network structure and design. This will allow the administrator to identify key systems which need to be better protected. Password policies and access control lists should be reviewed and backups and secure storage systems should be reviewed. This will allow the administrator to identify any possible problems related to recovery of important data in case of failure.

Cryptography

Cryptography is a very useful tool in the hands of a security designer. Typically, it allows two people to communicate over an unsecure network such as the Internet. Cryptography can add the ability to verify that the sender of a message is indeed who he claims to be, and also to encrypt the message itself, so that only the receiver (or number of receivers) can read

it. This is a very useful security measure when two nodes interact with each other with mutual trust. However, cryptography is not a solution for all securities in many applications, for example, VPN may use appropriate secure cryptography but it does not stop the hackers from guessing the password, a web application using SSL (Secure HTTP/HTTPS) can still have cross-site scripting, SQL injection, and other vulnerabilities. These security issues can still be exploited by attackers on a “secure website” just because secure in this case means that the connection between the attacker and the web server is encrypted and cannot be eavesdropped. In fact, an attacker will probably prefer attacking a web application over HTTPS than over HTTP just because his attacks cannot easily be caught using protocol analyzers or network intrusion detection systems such as Snort [15].

Digital Signature

For sending the information like legal documents, credit card payments, and letters, a cryptographic method known as digital signature is used as a means to verify the sender's identification. One of the widely acceptable application of digital signature is public key certification, as it certifies that a public key belongs to a specific entity. Public key certification is used in many popular secure networking protocols including IPsec and SSL. Binding a public key to a particular entity is usually done by a Certification Authority (CA). CA is responsible for verifying the entity (a person, router, host, and so on) and validating the identities, creates a certificate that binds the public key of the entity to identity.

Minimizing Impact—Detecting the Attack

A well-configured intrusion detection system together with log analysis allows network administrators to be alert when someone takes a fancy in probing their network. In fact, monitoring is a very good solution to the targeted attack problem. However, most of the time, the problem with monitoring is the overflow of information. For example, a default installation of Snort on a busy network will start generating various alerts, most of which are not relevant and are allowed traffic. A host-based intrusion detection system that is well configured, will allow the administrator to detect any servers or workstations that are misbehaving.

Incident Response Team

Just detecting an attack is obviously not enough in any organization, it needs to react to the attack. The job of the incident response team (IRT) is to react to the situation rationally and in a timely fashion as well as help fix the security problems exploited in the first place. In smaller organizations, the IRT would probably consist of selected individuals from different departments such as network administrators and human resources. The team has to be

skilled and trained to handle various situations—including identifying a targeted attack and reacting to it. In this case, the team might probably have to work with the legal department depending on the case. The IRT has to be highly skilled in decision making and reacting to such complex situations and often requires decisions to be taken in only a few seconds.

Containment

Various attacks can be employed by an attacker on the internal network using ARP spoofing that allows the attacker to view traffic between different hosts on the same physical network segment. Any clear text traffic such as passwords (e.g., HTTP basic authentication) or traffic (such as transfer of files through Windows network shares) can be viewed by making use of this attack. There are similar attacks to achieve the same kind of access—such as DNS spoofing or MAC address flooding, passwords are frequently shared across different servers and services. Guessing one password means that the attacker gains access to various other accounts by the same user. Less secure servers are easily accessible once inside the internal network.

RESPONDING TO CYBER ATTACKS

The critical flow of information out of flow of exchange is determined by a number of factors like regulatory requirements, liability obligations, and market signals (e.g., risk-related information through which the performance of a network may be influenced). Each national networked relationship may operate with its own unique set of additional factors. Policymakers may further shape certain factors to influence entity behavior and performance. It may be possible, for example, to strengthen the influence of market-related factors by using government procurement policies.

Develop Mechanisms to Respond to Cyber Incidents Leading to Cyber Attack

Organizational forms have been developed at multiple levels to investigate, analyze, and respond to cyber-security incidents. CERTs, for example, are becoming the critical backbone for preparing for and responding to cyber incidents of all types. These bodies differ in size and geographic scope and are in varying stages of development in industrialized and developing economies. To date, they are most developed in the financial services and public utilities sectors. Because CERTs are critical hubs for many types of information flows involving a wide range of incidents and different participants, it is critical that they engage in effective collaboration with their counterparts worldwide and develop procedures for managing incidents with a significant international dimension.

Effective cyber security will depend on strengthening and reinforcing the mechanisms of risk assessment and management within and among companies, organizations, government departments, and agencies. Significant threat indicators are likely to emerge only by accumulating, correlating, and analyzing incident-related data at the enterprise level or by analyzing information collected by a range of computer security incident response teams in multiple countries [12,16].

In countries with a long tradition of state involvement or ownership in key infrastructure sectors, such as France, for example, government officials are likely to take a much more top-down, state-directed approach to cyber security, which may inhibit them from entrusting responsibility for risk assessment to corporate executives. In contrast, the Indian Ministry of IT and CERT-In appear to attach high priority to improving risk management at the enterprise level. The presentations focus on enterprise security architectures and risk management policies.

CYBERETHICS

There are many constraints like laws of civil society, social pressure of the community in which we live. In general, four components of an ethical norm has been introduced and widely accepted that regulate our behavior in real life. These are law, social norms, market, and architecture. *Laws* are imposed by the government via the rules that are imposed through ex post sanctions. *Social norms* are defined as expressions of the community that usually have a well-defined sense of normalcy via some accepted standards of behavior. The *market regulates* through the price for goods and services or even for labor. The *architecture regulates* many physical constraints on our behavior (whether natural or human made) and is self-enforcing, self-executing. Some of the material presented here is derived from Refs. [21,22].

In cyberspace, we can see these four components of ethical norm in one way or the other that need to be either introduced or enforced. The law that provides protection against copyright, patent, regulates behavior by proscribing certain activities and by imposing ex post sanctions for violators. We need to define social norms within community that will regulate the behavior including Internet etiquette and social customs. The community will rely on shame and social stigma to enforce cultural norms. The market component can be implemented in a number of ways like advertisement of products via websites, pricing policies of Internet service providers, and so on. The architecture component is implemented via software code that is programs and protocols that make up Internet. These programs are usually known as architectures of cyberspace while code determines the way of accessing websites on Internet via username and password. All these four components together define cyberspace ethics or cyberethics.

CYBERSPACE REGULATION

The Internet's popularity and commercialization has led to some familiar social problems and conflicts in cyberspace including, violation of privacy, emergence of perverted forms of speech, illegitimate copying of music and video files, unsolicited e-mail (spam), and many others. Although the marketplace always functions as a very critical constraint on the behavior, it should take more appropriate steps to check on these issues instead of giving more emphasis to regulatory entities like law, social norms, and architectural code.

In order to regulate the cyberspace, governments may pursue other forms of Internet regulation such as regulation of information infrastructure or regulation of e-commerce, regulation of privacy or data protection via certain security standards for a website, etc.

The European Union Privacy Directive has defined strict rules for the companies doing business within European Union. The United States mainly adapts the self-regulation policies for companies.

There have been some efforts made globally to harmonize laws pertaining to Internet. For example, WIPO Copyright Treaty, which stipulates how copyright laws will be applied to digital works. Although harmonization looks a reasonable theoretical concept, it will be difficult to accomplish in practice due to embedded cultural and legal differences between countries. It would be good if countries can work on defining policy interoperability instead of harmonization thus agreeing on what goals of policy should achieve with a determination of its implementation.

Although there is some disagreement on how the Internet should be regulated through government interventions, Net will not be able to survive without any type of mutual coordination among the governments. The major responsibilities of governing bodies include technical support and determination of standards and management of domain names and IP addresses.

CYBER STANDARDS ORGANIZATIONS

There are two major governing bodies as World Wide Web Consortium: an international standards setting body and IETF that develops technical standards of protocols. The DNS maps the domain names of the organizations to actual IP address and as such needs coordination. It is a hierarchical system divided into separate domains. The Internet application browser forwards the domain name to DNS server which is normally operated by ISP and the server locates the databases for each of the subdomains.

The system was formerly administered by a small private company known as NSI. Looking at the exponential growth of Internet and under political pressure, the system was handed over to ICANN which is an international non-profit organizations with full responsibilities of DNS. It does not allocate domain names but defines the policies and

procedures for domain name distribution and has the final say in selecting any firm for the name. The names are allocated by another organization as VeriSign.

Acknowledgments

Thanks to many of my graduate students who, while taking my course, helped me in the preparation of this chapter in one way or the other. In particular, my special thanks goes to Rakesh Dontula, Sandhya Police, Harideep Jonnalagadda, and Lakshmi Madhavi Potlapalli who help me in getting the information and drawing figures in time.

References

1. Microsoft, Security essential. <http://www.microsoft.com/en-us/securityessentials/default.aspx> (accessed on January 12, 2010).
2. B. Forouzan, *TCP/IP Protocol Suite*, 3rd edn., McGraw-Hill, New York, 2006.
3. H. F. Lipson, Tracking and tracing cyber-attack: "Technical challenges and global policy issues", CERT Coordinator, November 2002, Special reference, CMU/SEU-2002-SR-009.
4. Internet Society, Brief history of the internet and related networks, 2006. <http://www.isoc.org/intenet/history/cerf.shtml> (accessed on April 10, 2011).
5. G. S. Hura and M. Singhal, *Data and Computer: Networking and Internetworking*, CRC Press, Boca Raton, FL, 2001.
6. GFI End Point Security, White paper. <http://www.gfi.com/end-pointsecurity/esecpapers.htm> (accessed on May 20, 2010).
7. G. S. Hura, Guest editor of special issue on Internet: State-of-the-art, *Computer Communication*, 20(16), 1391–1540, 1998.
8. Internet Systems Consortium, Downloads, 2006. <http://www.isc.org/software/bind/documentation> (accessed on April 10, 2011).
9. National Coordinating Center for Telecommunications, Resources. <http://www.ncs.gov/ncc/govind.html> (accessed on May 21, 2010).
10. National Institute of Standards and Technology, *An Introduction to Computer Security, The NIST Handbook*. Special Publication, 2006, Technology Administration, U.S. Department of Commerce. <http://csrc.nist.gov/groups/SMA/fisma/index.html> (accessed on December 22, 2009).
11. *Cert-In Workshop on Information Security Policies and Procedure*, 2006, New Delhi, September 3, 2004. <http://www.certain.org.in/knowledgebase/presentation> (accessed on May 20, 2010).
12. United States Computer Emergency Readiness Team, National cyber alert systems, 2006. <http://www.uscert.gov/cas/techalerts/TA09-088A.html> (accessed on 10 April 10, 2011).
13. *The Imperatives of National Cyber Security and Cyber Security in the International Context*, Washington, DC, 2005. <http://web.worldbank.org/website/external/topics/extinformat10andcommunicationandtechnologies/0..contentMDK:20690461~menuPK:282842~pagePK:210058~piPK:210062~theSitePK:282823.00.html> (accessed on April 10, 2011).
14. SourceFire, Snort users manual, 2006. http://www.snort.org/assets/166/snort_manual.pdf (accessed on April 10, 2011).

15. M. Dunn and I. Wigert, *The Critical Information Infrastructure Prevention (CIIP) Handbook 2004*, A. Wenger and J. Metzger (eds.), Swiss Federal Institute of Technology, 2006. <http://www.isn.ethz.ch/isn/Digital-Library/Publications> (accessed on April 10, 2011)
16. A. Wong and A. Yeung, *Network Infrastructure Security*, Springer Verlag, Berlin, Germany, 2009.
17. Dartmouth College Institute for Security, Technology and Society, Technical reports presentations, 2006. http://info.ists.dartmouth.edu/library/list_presentations_and_tech_reports (accessed on April 10, 2011).
18. Department of Homeland Security, *A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment*, 2006. <http://www.dhs.gov/dhspublic/interapp>
19. Antiphishing Org, Consumer advise on phishing, 2006. <http://www.antiphishing.org/resourees.html> (accessed on April 10, 2011).
20. L. Applegat, E-business models, in *Information Technology and the Future of the Enterprise*, G. Dickson and G. DeSanctis (eds.), Prentice Hall, Upper Saddle River, NJ, pp. 49–101, 2001.
21. R. Spinello, *Cyberethics: Morality and Law in Cyberspace*, Jones and Bartlett Publishers, Sudbury, MA, 2006.